



# **Multi-Protocol Label Switching (MPLS) Conformance and Performance Testing**



# Table of Contents

|                                                                |    |
|----------------------------------------------------------------|----|
| Abstract .....                                                 | 4  |
| Introduction .....                                             | 4  |
| What is MPLS? .....                                            | 5  |
| Historical perspective .....                                   | 5  |
| MPLS and IP .....                                              | 5  |
| Advantages of MPLS .....                                       | 6  |
| How Does MPLS Work? .....                                      | 6  |
| How Is MPLS Used? .....                                        | 9  |
| MPLS Challenges .....                                          | 15 |
| Why Test for MPLS Conformance? .....                           | 16 |
| Why Test for MPLS Scalability and Performance? .....           | 16 |
| Test Solution Requirements .....                               | 17 |
| Ixia's Approach to MPLS Testing .....                          | 19 |
| MPLS conformance testing .....                                 | 19 |
| MPLS scalability and performance testing .....                 | 19 |
| Conclusion .....                                               | 21 |
| Appendix: MPLS Testing Examples .....                          | 22 |
| IxANVL LDP Conformance Test .....                              | 22 |
| IxScriptMate L2 VPN Partial Mesh Performance Test .....        | 23 |
| IxScriptMate L3 VPN RSVP-TE Egress Performance .....           | 24 |
| IxExplorer LDP Extended Martini Session Scalability Test ..... | 25 |
| IxScriptMate VPLS MAC Address Cache Capacity Test .....        | 27 |
| IxExplorer RSVP-TE Fast Reroute Test .....                     | 28 |
| Glossary .....                                                 | 29 |

**Today's  
communication  
networks and  
services are  
migrating to a  
converged paradigm  
centered on IP  
(Internet Protocol).**

## Abstract

Today's communication networks and services are migrating to a converged paradigm centered on IP (Internet Protocol). MPLS (Multi-Protocol Label Switching) has emerged as a key enabling technology for this migration. MPLS technology has proven its value for delivering new services while at the same time allowing migration from old to new networks. The rollout of MPLS brings the challenges associated with any new networking technology — validating proper conformance with industry standards prior to production deployment and verifying acceptable performance. This white paper provides an overview of MPLS, and Ixia's approach to testing and validating that technology.

## Introduction

Several forces shape the current worldwide communications landscape. One is the general economic slowdown since early 2000, in particular, the pop of the telecommunications industry bubble. Another is the much-ballyhooed convergence of digital communications networks (voice, video, data) and the emergence of IP as the protocol of choice. Finally, globalization and deregulation have combined to level the playing field and increase competitive pressures.

The economic slowdown of recent years and resulting over-capacity in core networks has forced service providers and carriers to look seriously at their return on investment from network assets. With pure bandwidth becoming, in essence, a commodity, industry focus has shifted to supplying the value-add services customers need. As new technologies are adopted, the provider's ability to consolidate disparate existing networks is a key to deploying all services, old and new, profitably. The enterprise market has shown a similar response to the slowdown — increasing efficiencies by pragmatically applying the new technologies that make such improvements possible.

Consequently, MPLS has great appeal for telecommunications providers. It can handle a variety of services, both legacy and new, over a single network. It enables higher-value applications and services to be delivered from the service provider's network, thereby reducing requirements on customer-premises equipment. Integration and consolidation speak loudly in today's business environment.

It's clear that the migration to MPLS is well under way. Every major carrier in the US, and many internationally, have deployed or announced plans for MPLS backbones. A 2003 study by Infonetics Research shows 62 percent of service providers are now engaged in some form of data network convergence over IP or IP/MPLS, with 86 percent doing so in 2004. Since legacy services, such as Frame Relay and ATM, can be carried over the MPLS network, this network convergence is often transparent to the end user enterprise. Moving forward, newer low cost services such as Ethernet will drive further adoption.

Beyond large carrier networks, MPLS is also finding its way into the larger enterprise networks of organizations such as retailers, investment companies, government agencies and the military, health care organizations, and technology enterprises.

# What is MPLS?

## Historical perspective

MPLS is based on the concept of label switching: an independent and unique “label” is added to each data packet and this label is used to switch and route the packet through the network. The label is simple — essentially a short hand version of the packet’s header information — so network equipment can be optimized around processing the label and forwarding traffic. This concept has been around the data communications industry for years. X.25, Frame Relay, and ATM are examples of label switching technologies.

Several label switching initiatives emerged in the mid-1990’s to improve the performance of software-based IP routers and provide Quality of Service (QoS).

Among these were IP Switching (Ipsilon/ Nokia), Tag Switching (Cisco), and ARIS (IBM). In early 1997, an Internet Engineering Task Force (IETF) Working Group was chartered to standardize a label switching technology. MPLS emerged from this effort as another labeling scheme, but one with this distinct advantage: it uses the same routing and host addressing schemes as IP — the protocol of choice in today’s networks. Today MPLS is defined by a set of IETF Request for Comments (RFCs) and draft specifications (under development).

## MPLS and IP

It is important to understand the differences in the way MPLS and IP routing forward data across a network. Traditional IP packet forwarding uses the IP destination address in the packet’s header to make an independent forwarding decision at each router in the network.

These hop-by-hop decisions are based on network layer routing protocols, such as Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP). These routing protocols are designed to find the shortest path through the network, and do not consider other factors, such as latency or traffic congestion.

MPLS creates a connection-based model overlaid onto the traditionally connectionless framework of IP routed networks. This connection-oriented architecture opens the door to a wealth of new possibilities for managing traffic on an IP network. MPLS builds on IP, combining the intelligence of routing, which is fundamental to the operation of the Internet and today’s IP networks, with the high performance of switching. Beyond its applicability to IP networking, MPLS is being expanded for more general applications in the form of Generalized MPLS (GMPLS), with applications in optical and Time-Division Multiplexing (TDM) networks.

**MPLS is based on the concept of label switching: an independent and unique “label” is added to each data packet and this label is used to switch and route the packet through the network.**

**MPLS is a technology used for optimizing traffic forwarding through a network.**

## Advantages of MPLS

- MPLS enables a single converged network to support both new and legacy services, creating an efficient migration path to an IP-based infrastructure. MPLS operates over both legacy (DS3, SONET) and new infrastructure (10/100/1000/10G Ethernet) and networks (IP, ATM, Frame Relay, Ethernet, and TDM).
- MPLS enables traffic engineering. Explicit traffic routing and engineering help squeeze more data into available bandwidth.
- MPLS supports the delivery of services with Quality of Service (QoS) guarantees. Packets can be marked for high quality, enabling providers to maintain a specified low end-to-end latency for voice and video.
- MPLS reduces router processing requirements, since routers simply forward packets based on fixed labels.
- MPLS provides the appropriate level of security to make IP as secure as Frame Relay in the WAN, while reducing the need for encryption on public IP networks.
- MPLS VPNs scale better than customer-based VPNs since they are provider-network-based, reducing the configuration and management requirements for the customer.

## How Does MPLS Work?

MPLS is a technology used for optimizing traffic forwarding through a network.

Though MPLS can be applied in many different network environments, this discussion will focus primarily on MPLS in IP packet networks — by far the most common application of MPLS today.

MPLS assigns labels to packets for transport across a network. The labels are contained in an MPLS header inserted into the data packet (Figure 1).

These short, fixed-length labels carry the information that tells each switching node (router) how to process and forward the packets, from source to destination. They have significance only on a local node-to-node connection. As each node forwards the packet, it swaps the current label for the appropriate label to route the packet to the next node. This mechanism enables very-high-speed switching of the packets through the core MPLS network.

MPLS combines the best of both Layer 3 IP routing and Layer 2 switching. In fact, it is sometimes called a “Layer 2½” protocol. While routers require network-level intelligence to determine where to send traffic, switches only send data to the next hop, and so are inherently simpler, faster, and less costly. MPLS relies on traditional IP routing protocols to advertise and establish the network topology. MPLS is then overlaid on top of this topology. MPLS predetermines the path data takes across a network and encodes that information into a label that the network’s routers understand. This is the connection-oriented approach previously discussed. Since route planning occurs ahead of time and at the edge of the network (where the customer and service provider network meet), MPLS-labeled data requires less router horsepower to traverse the core of the service provider’s network.

## MPLS routing

MPLS networks establish Label-Switched Paths (LSPs) for data crossing the network. An LSP is defined by a sequence of labels assigned to nodes on the packet's path from source to destination. LSPs direct packets in one of two ways: hop-by-hop routing or explicit routing.

**Hop-by-hop routing.** In hop-by-hop routing, each MPLS router independently selects the next hop for a given Forwarding Equivalency Class (FEC). A FEC describes a group of packets of the same type; all packets assigned to a FEC receive the same routing treatment. FECs can be based on an IP address route or the service requirements for a packet, such as low latency.

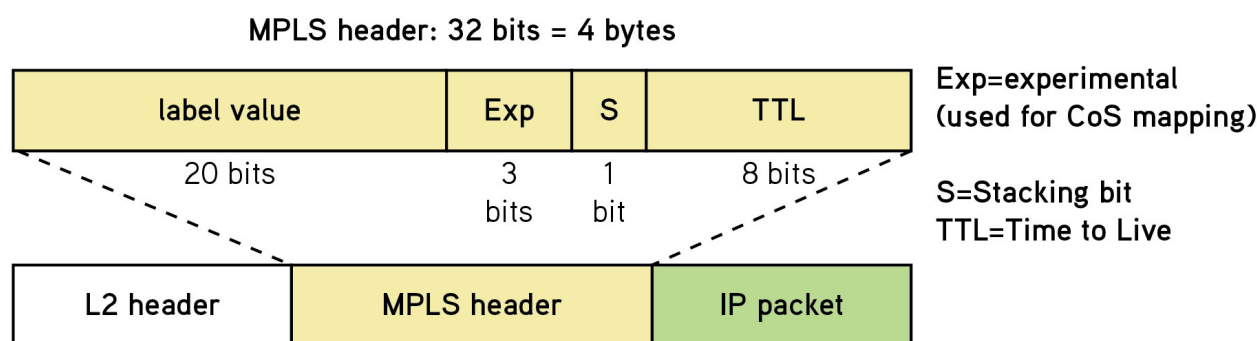


Figure 1. MPLS header format on an MPLS packet.

In the case of hop-by-hop routing, MPLS uses the network topology information distributed by traditional Interior Gateway Protocols (IGPs) — routing protocols such as OSPF or IS-IS. This process is similar to traditional routing in IP networks, and the LSPs follow the routes the IGPs dictate.

**Explicit routing.** In explicit routing, the entire list of nodes traversed by the LSP is specified in advance. The path specified could be optimal or not, but is based on the overall view of the network topology and, potentially, on additional constraints. This is called Constraint-Based Routing.

Along the path, resources may be reserved to ensure QoS. This permits traffic engineering to be deployed in the network to optimize use of bandwidth.

**Label Information Base.** As the network is established and signaled, each MPLS router builds a Label Information Base (LIB)—a table that specifies how to forward a packet. This table associates each label with its corresponding FEC and the outbound port to forward the packet to.

This LIB is typically established in addition to the routing table and Forwarding Information Base (FIB) that traditional routers maintain.

In the case of hop-by-hop routing, MPLS uses the network topology information distributed by traditional Interior Gateway Protocols (IGPs) — routing protocols such as OSPF or IS-IS.

## Signaling and label distribution

Connections are signaled and labels are distributed among nodes in an MPLS network using one of several signaling protocols, including Label Distribution Protocol (LDP) and Resource reSerVation Protocol with Tunneling Extensions (RSVP-TE).

Connections are signaled and labels are distributed among nodes in an MPLS network using one of several signaling protocols, including Label Distribution Protocol (LDP) and Resource reSerVation Protocol with Tunneling Extensions (RSVP-TE). Alternatively, label assignment can be piggybacked onto existing IP routing protocols such as BGP.

The most commonly used MPLS signaling protocol is LDP. LDP defines a set of procedures used by MPLS routers to exchange label and stream mapping information. It is used to establish LSPs, mapping routing information directly to Layer 2 switched paths. It is also commonly used to signal at the edge of the MPLS network — the critical point where non-MPLS traffic enters. Such signaling is required when establishing MPLS VPNs, for example.

RSVP-TE is also used for label distribution, most commonly in the core of networks that require traffic engineering and QoS. A set of extensions to the original RSVP protocol, RSVP-TE provides additional functionality beyond label distribution, such as explicit LSP routing, dynamic rerouting around network failures, preemption of LSPs, and loop detection. RSVP-TE can distribute traffic engineering parameters such as bandwidth reservations and QoS requirements.

Multi-protocol extensions have been defined for BGP, enabling the protocol to also be used to distribute MPLS labels. MPLS labels are piggybacked onto the same BGP messages used to distribute the associated routes.

MPLS allows multiple labels (called a label stack) to be carried on a packet. Label stacking enables MPLS nodes to differentiate between types of data flows, and to set up and distribute LSPs accordingly. A common use of label stacking is for establishing tunnels through MPLS networks for VPN applications.

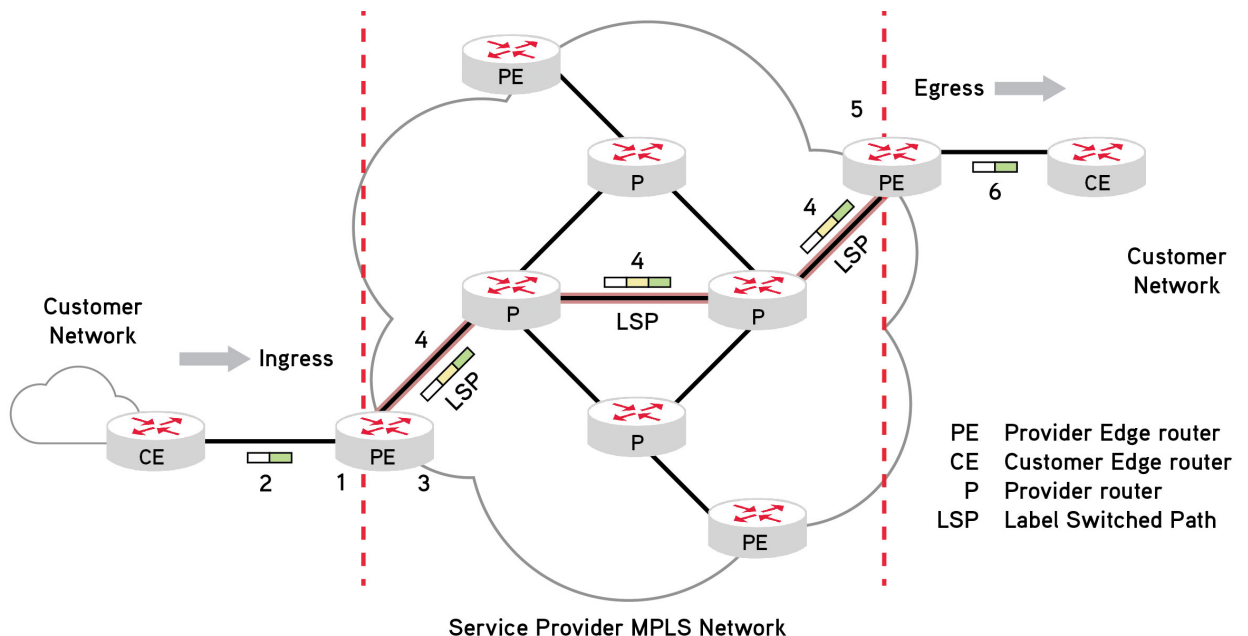


Figure 2. MPLS network.

## Data flow in an MPLS network

Figure 2 shows a typical MPLS network and its associated elements. The central cloud represents the MPLS network itself. All data traffic within this cloud is MPLS- labeled. All traffic between the cloud and the customer networks is not MPLS- labeled (IP for example). The customer- owned Customer Edge (CE) routers interface with the Provider Edge (PE) routers (also called Label Edge Routers, or LERs) owned by the service provider. At the ingress (incoming) side of the MPLS network, PE routers add MPLS labels to packets. At the egress (outgoing) side of the MPLS network, the PE routers remove the labels. Within the MPLS cloud, P (Provider) routers (also called Label Switching Routers, or LSRs), switch traffic hop-by-hop based on the MPLS labels.

To demonstrate an MPLS network in operation, we will follow the flow of data through the network in Figure 2:

1. Before traffic is forwarded on the MPLS network, the PE routers first establish LSPs through the MPLS network to remote PE routers.
2. Non-MPLS traffic (Frame Relay, ATM, Ethernet, etc.) is sent from a customer network, through its CE router, to the ingress PE router operating at the edge of the provider's MPLS network.
3. The PE router performs a lookup on information in the packet to associate it with a FEC, then adds the appropriate MPLS label(s) to the packet.
4. The packet proceeds along its LSP, with each intermediary P router swapping labels as specified by the information in its LIB to direct the packet to the next hop.
5. At the egress PE, the last MPLS label is removed and the packet is forwarded by traditional routing mechanisms.
6. The packet proceeds to the destination CE and into the customer's network.

## How Is MPLS Used?

One of the primary original goals of MPLS, boosting the performance of software- based IP routers, has been superseded as advances in silicon technology have enabled line-rate routing performance implemented in router hardware. In the meantime, additional benefits of MPLS have been realized, notably VPN services and traffic engineering.

## Virtual Private Networks

A Virtual Private Network (VPN) is a private network service delivered over a public (shared) network. VPNs benefit end customers by allowing remote locations to be securely connected over a public network, without the expense of buying or leasing dedicated network lines. MPLS enables VPNs by providing a circuit-like, connection-oriented framework, allowing carriers to deploy VPNs over the traditionally connectionless IP network infrastructure.

One of the primary original goals of MPLS, boosting the performance of software- based IP routers, has been superseded as advances in silicon technology have enabled line-rate routing performance implemented in router hardware.

**MPLS VPNs are maintained on the service provider's equipment, which can provide significant cost savings and increased scalability compared with other VPN technologies.**

**MPLS VPNs vs. IPsec VPNs.** The term VPN can be confusing, as it is used to describe a number of technologies. VPNs can be organized into two broad categories:

- Customer-based: the VPN is configured exclusively on customer- located equipment and uses tunneling protocols across the public network, most commonly IPsec.
- Network-based: the VPN is configured on service provider equipment and managed by the provider. MPLS VPNs are an example of network-based VPNs.

IPsec adds secure encryption capabilities to IP. It is typically managed by the end customer, outside of a service provider's network, where there is a higher degree of exposure to breaches of data privacy.

IPsec is especially useful for securing remote location VPN connections back to the corporate network.

MPLS VPNs are maintained on the service provider's equipment, which can provide significant cost savings and increased scalability compared with other VPN technologies. MPLS VPNs keep different customers' traffic separated by uniquely identifying each VPN flow and setting up circuit-like connections. This mechanism provides traffic separation and is transparent to end users within the VPN group. MPLS VPNs provide security inherently, essentially making IP as secure as Frame Relay or ATM, and reducing the need for encryption. Miercom, an independent network consultancy and testing laboratory, tested MPLS VPN security on a network of various routers, and concluded (2001): "Our test results have demonstrated that MPLS-based VPN networks offer the same level of security as Frame Relay or ATM."

**L3 VPNs.** MPLS VPNs fall into two broad classes — those that operate at Layer 3 and those that operate at Layer 2. Layer 3 VPNs were first to be investigated and standardized in RFCs. Layer 3 VPNs based on RFC 2547bis have seen the most widespread deployment to date.

RFC 2547bis-based Layer 3 VPNs use extensions to BGP, specifically Multi- Protocol internal BGP (MP-iBGP), to distribute VPN routing information across the provider backbone. Standard MPLS mechanisms (as previously discussed) are used to forward the VPN traffic across the backbone. In an L3 VPN, the CE and PE routers are IP routing peers. The CE router provides the PE router with the routing information for the customer's private network behind it. The PE router stores this private routing information in a Virtual Routing and Forwarding (VRF) table; each VRF is essentially a private IP network. The PE router maintains a separate VRF table for each VPN, thereby providing appropriate isolation and security. VPN users have access only to sites or hosts within the same VPN. In addition to the VRF tables, the PE router also stores the normal routing information it needs to send traffic over the public Internet.

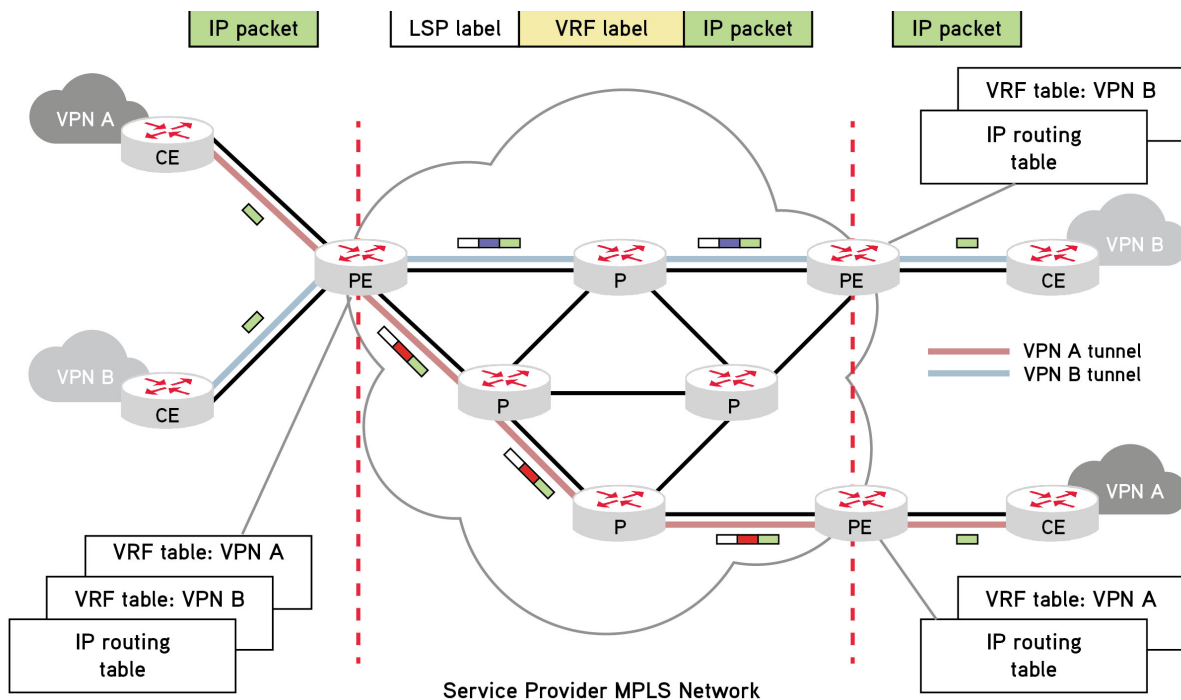


Figure 3. Layer 3 VPN MPLS network.

L3 VPNs use a two-level MPLS label stack (see Figure 3). The inner label carries VPN- specific information from PE to PE. The outer label carries the hop-by-hop MPLS forwarding information. The P routers in the MPLS network only read and swap the outer label as the packet passes through the network. They do not read or act upon the inner VPN label — that information is tunneled across the network.

The L3 VPN approach has several advantages. The customer IP address space is managed by the carrier, significantly simplifying the customer IT role — as new customer VPN sites are easily connected and managed by the provider. L3 VPNs also have the advantage of supporting auto-discovery by leveraging the dynamic routing capabilities of BGP to distribute VPN routes.

The Layer 3 approach has disadvantages as well. Layer 3 VPNs support only IP or “IP-encapsulated” customer traffic. Scaling also can be a significant issue with PE routers required to support BGP routing tables that are larger than normal with the addition of the VPN routes.

**L2 VPNs.** Layer 2 MPLS VPNs have recently generated much interest from carriers and vendors and are beginning to be deployed (2003). Layer 2 MPLS VPN standards are still in the development phase, but the industry has centralized on the IETF Martini drafts, named after primary author Luca Martini. These drafts define a method for setting up L2 VPN tunnels across an MPLS network that can handle all types of Layer 2 traffic, including Ethernet, Frame Relay, ATM, TDM, and PPP/HDLC.

There are two kinds of Layer 2 VPNs that use the Martini methodology:

- Point-to-point: similar to ATM and Frame Relay using fixed, point-to-point connections (LSPs) across the network.
- Multi-point: supporting meshed and hierarchical topologies.

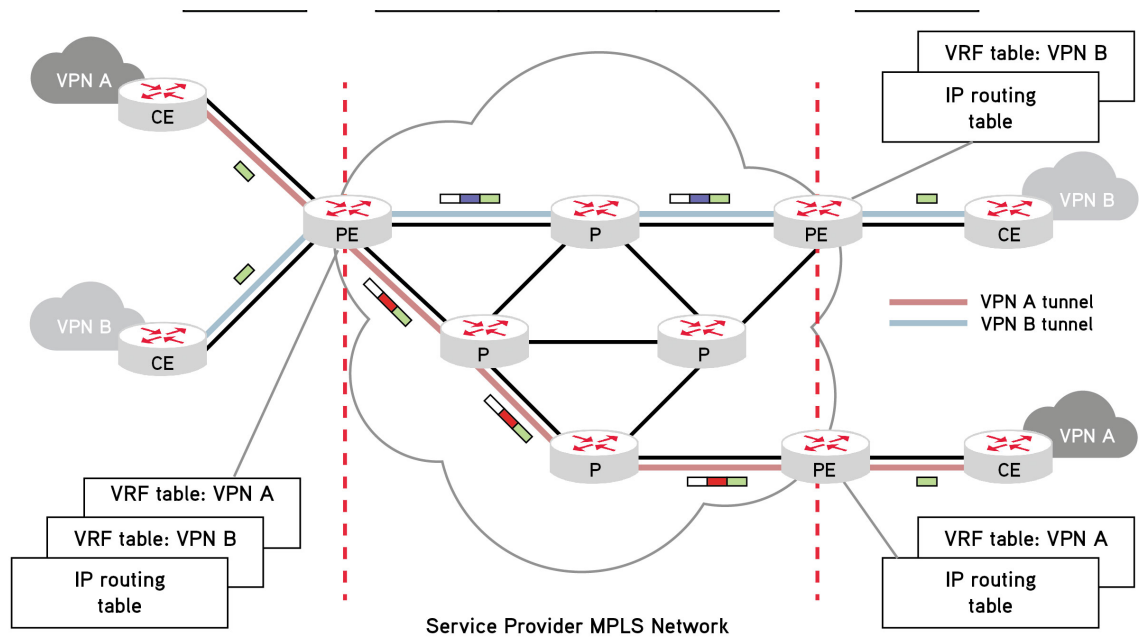


Figure 4. Layer 2 VPN MPLS network.

**VPLS (Virtual Private LAN Services) is a multi-point L2 VPN model that has generated significant interest of late.**

VPLS (Virtual Private LAN Services) is a multi-point L2 VPN model that has generated significant interest of late. VPLS uses Ethernet as the access technology between the customer and the provider network and enables a private corporate Ethernet network to be extended over a provider-managed MPLS infrastructure.

Multiple corporate customer sites can be connected together with all locations appearing to be on the same Layer 3 network, all without the complexity of configuring Layer 3 routers.

In Layer 2 VPNs, the PE and CE routers need not be routing peers as required in Layer 3 VPNs. Instead, only a Layer 2 connection needs to exist between PE and CE, with the PE routers simply switching incoming traffic into tunnels configured to one or more other PE routers. A Layer 2 MPLS VPN determines reachability through the data plane by using address learning, in contrast with Layer 3 VPNs, which determine reachability through the control plane by exchanging BGP routes.

L2 VPNs use label stacking similar to Layer 3 VPNs. The outer tunnel label determines the hop-by-hop path through the network.

The inner Virtual Circuit (VC) label identifies the VLAN, VPN, or connection at the end point. In addition, there is an optional Control Word following the VC label that carries information about the enclosed Layer 2 packet.

Layer 2 MPLS VPNs have the distinct advantage of being able to transport any enterprise protocol — whatever is being carried is transparent to the MPLS network. They can also run over nearly any transport medium, including ATM, Frame Relay, Packet over SONET, and Ethernet, enabling the integration of connectionless IP networks with connection-oriented networks. End customer expertise is minimal since no routing configuration is required.

On the downside, L2 VPNs may not scale as well as L3 VPNs. A full mesh of LSPs must be set up between all L2 VPN sites, a requirement that does not scale well with large numbers of sites. In addition, they cannot take advantage of automatic route discovery available with L3 VPNs, and so are better suited to situations with a smaller number of VPN sites and static routes.

## QoS/CoS

One of the key shortcomings of IP-based networks, compared with Frame Relay and ATM networks, has been their inability to provide service guarantees for traffic. For example, real-time traffic such as voice or video needs high quality service (low latency, low jitter, etc.) to successfully traverse a network. Similarly, mission-critical data, such as e-commerce transactions, must have priority over normal web browser traffic.

MPLS's connection-oriented nature provides the framework necessary to give quality guarantees to IP traffic. While QoS and Class of Service (CoS) are not fundamental features of MPLS, they can be applied in MPLS networks where traffic engineering is used. This enables providers to establish Service Level Agreements (SLAs) with customers to guarantee service aspects such as network bandwidth, delay, and jitter. Value-added services can be delivered in addition to basic data transport, increasing revenue propositions and ultimately enabling the move to converged networks.

**IntServ and DiffServ.** Several mechanisms have developed over time to establish QoS/CoS within a network. In the IntServ (Integrated Services) model, RSVP was developed to signal QoS requirements across a network, allowing devices to negotiate and establish guaranteed traffic parameters such as bandwidth and latency end-to-end. It uses hard allocation of resources, guaranteeing services down to a per-flow basis. The DiffServ (Differentiated Services) model is less stringent, providing for CoS delivery by classifying traffic into relative priority levels for aggregate treatment, but without signaling or end-to-end guarantees of service. DiffServ redefines the Type of Service (TOS) field in the IP packet header to provide this classification.

While IntServ offers traffic bandwidth guarantees, it has proved to be not very scalable or practical to operate across large networks. The DiffServ architecture, on the other hand, is a scalable alternative, but does not provide guarantees. Recent work in the IETF has focused on combining DiffServ and MPLS traffic engineering elements to provide QoS guarantees in MPLS packet networks. The DiffServ information in IP packet headers is mapped into the label information of the MPLS packets. MPLS routers act upon the prioritization information in the packets to forward the data appropriately. Some of the mechanisms used include traffic shaping, queuing, and packet classification.

QoS is typically implemented at the edge of the MPLS cloud, where non-labeled traffic from the customer network enters the carrier network. At this entry point for example, delay-sensitive real-time traffic, such as IP voice or video conferencing traffic, can be prioritized for delivery over bulk data transmissions.

One of the key shortcomings of IP-based networks, compared with Frame Relay and ATM networks, has been their inability to provide service guarantees for traffic.

## Traffic engineering

Another key shortcoming of IP, especially in public networks, is its inability to optimize network resource utilization. Using standard IP routing, all traffic between two points is sent over the shortest path even though multiple paths may exist. During periods of high traffic volume, this can result in traffic congestion on certain routes while alternative routes are underused. This is known as the hyper-aggregation problem (Figure 5).

Rather than adding bandwidth to handle traffic volume increases, MPLS traffic engineering uses existing bandwidth more efficiently by allowing packets to be routed along explicit routes and with specific bandwidth guarantees.

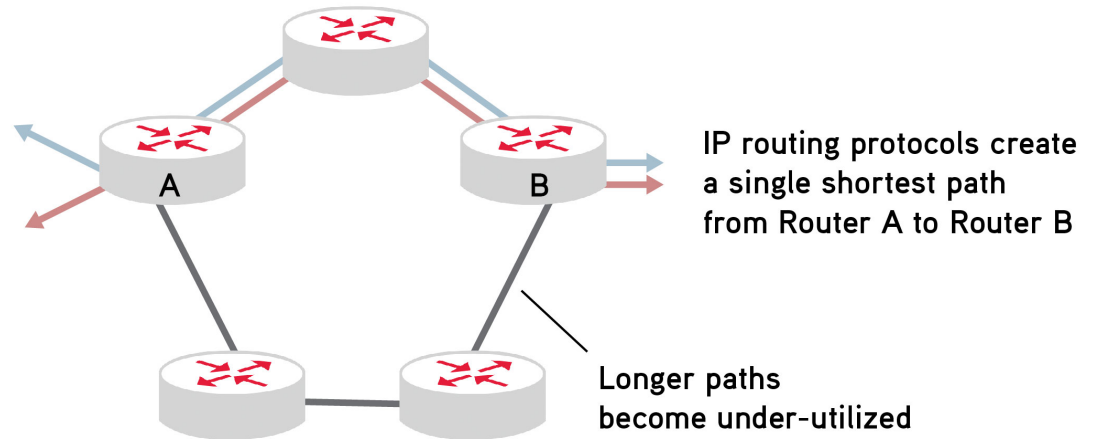


Figure 5. Hyper-aggregation in conventional IP networks.

**Another key shortcoming of IP, especially in public networks, is its inability to optimize network resource utilization.**

This is known as Constraint-Based Routing and is the key to MPLS traffic engineering. Constraint-Based Routing manages traffic paths within an MPLS network, allowing traffic to be steered to desired paths.

MPLS traffic engineering also enables resiliency and reliability to be built into carrier networks, increasing the availability and value of the network to their customers. Using MPLS traffic engineering, LSP connections can be optimized and preempted. When outages occur, traffic can be actively rerouted around failed links. An example of this is RSVP-TE Fast Reroute, which provides for sub-50ms switchovers between primary and back up LSPs or LSP bundles.

Traffic engineering is deployed in MPLS networks via traffic engineering extensions to IGPs, such as OSPF and IS-IS. OSPF-TE and IS-IS-TE carry additional information —such as link bandwidth, link utilization, delay, priority, preemption, etc. — to allow the network to utilize paths that meet service requirements, resource availability, load balancing, and failure recovery objectives. RSVP-TE is widely used for MPLS signaling in networks that require traffic engineering.

MPLS traffic engineering is typically deployed in the core of the MPLS network, while QoS is used at the edge. QoS at the edge ensures that high priority packets get preferential treatment, while traffic engineering avoids network congestion and appropriately utilizes available bandwidth resources. Together, QoS and traffic engineering enable organizations to move away from multiple, specialized networks for voice, video, and data to a single converged IP/MPLS network, dramatically reducing overhead and cost.

## MPLS Challenges

MPLS has made significant progress over the last few years and is well into mainstream deployment in networks around the world. But key challenges to attaining more widespread acceptance remain. MPLS encompasses a wide range of functionality and applications, therefore its implementation has an associated high level of complexity. Vendors who develop MPLS technology, as well as organizations looking at deploying MPLS in a network today, must also factor in MPLS's continually evolving state and its impact on network performance and scalability.

MPLS is not a standalone technology — it is overlaid on Layer 2 technologies such as Ethernet or ATM, and must operate in conjunction with other control plane protocols, such as IP routing. The complexity of MPLS deployments is increased because of this interaction. In some cases, four or more protocols may be involved in a given network scenario, necessitating careful coordination and validation of the end-to-end system. Integration of legacy services and deployment of new services, such as VPNs, requires tunneling, which in turn increases the setup requirements for a given circuit.

Though under development for a number of years, MPLS continues to evolve rapidly. The primary goals of the technology have shifted over time as technology has progressed. Today, a number of extensions to the MPLS protocols, as well as new functionality, are under development. New developments often obsolete older ones. This dynamic nature presents a moving target to those developing and deploying MPLS. Vendors must decide whether to implement a new feature with an eye on the industry's current direction. Service providers gauge the viability of new developments by asking whether they solve a given problem better. On certain issues, the industry has split into multiple camps, further complicating the situation as organizations trade off the long term risk of obsolescence with the shorter term benefits of implementing a certain technology. Interoperability of MPLS equipment in heterogeneous networks remains an issue and will continue to be so for several years to come.

Though advances in silicon technology have vastly improved the raw performance of today's routers, the complexity of MPLS in real network applications presents performance and scalability issues. The challenge is typically not in the MPLS core network, where data is simply being label-switched, but at the network edge where MPLS must integrate with non-MPLS networks, and where services are initiated. As networks converge, traffic loads increase and networks must be able to deal with the overhead of handling real-time and prioritized traffic. The meshed connections required for VPN deployments can quickly challenge equipment scalability limitations, as well as provisioning and management requirements. Large service provider networks have the ultimate scalability challenge and must consider the limitations of their equipment as they look to maximize return on investment.

The challenges presented by MPLS ultimately necessitate thorough testing and validation of MPLS systems during development and prior to deployment. MPLS is by no means a plug-and-play proposition. Performing appropriate due diligence is the only way to ensure success when dealing with a broad-scope and rapidly evolving technology such as MPLS.

**MPLS has made significant progress over the last few years and is well into mainstream deployment in networks around the world.**

**Equipment vendors find themselves at the leading edge of these challenges as they continually update their feature sets to the latest standards and options, while at the same time improving performance and scalability.**

## Why Test for MPLS Conformance?

MPLS standards and implementations are dynamic. At the time of this writing, there were over 100 IETF drafts associated with MPLS, and over 20 RFCs. In such a dynamic environment, standards compliance and the corresponding expectation of equipment interoperability present significant challenges.

Equipment vendors find themselves at the leading edge of these challenges as they continually update their feature sets to the latest standards and options, while at the same time improving performance and scalability. They must do this, both to remain competitive in their market and to meet the demands of their customers.

Development test and quality assurance groups therefore need an efficient way to verify the correctness of their implementations. Formalized conformance testing against standards supplies this confidence. Beyond ensuring product interoperability and quality, conformance testing can also accelerate product development by detecting bugs or correcting design issues early in the development cycle, thereby reducing the product's time to market and hence increasing profitability.

For both service providers and enterprise organizations, multi-vendor environments are the reality today. Such a reality is untenable without equipment interoperability driven by standards-based implementations. Networks are also dynamic, so when it comes time to upgrade, conformance and regression testing are crucial to ensure that new software releases do not break existing services.

To achieve adequate test coverage for compliance with a standard, hundreds of conformance test cases are typically necessary to cover a given protocol, and these tests must be appropriately updated as necessary. Since test cycles are often very frequent (daily in some cases), these tests must be automated as well. To address these challenges, most vendors and service providers rely on conformance testing products that are maintained and supported by a dedicated third-party.

## Why Test for MPLS Scalability and Performance?

After verifying the standards compliance and interoperability of an MPLS system, the next challenge is to determine the ability of an implementation to perform in a real network. Given the complexity of the protocols involved and the multi-layered nature of MPLS, scalability and performance are often genuine concerns. Equipment vendors typically test and publish the scalability and performance capabilities of their products. End users will often validate the numbers while additionally testing specific network scenarios unique to their deployment.

### Scalability

Scalability is typically viewed as the biggest challenge in service providers' MPLS networks today. They must understand the dynamics of growth in their networks as new customers are added, as well as the ultimate limits of their networks. Several metrics are key in determining scalability:

- Router capacity: The capacity of the MPLS routers to handle large numbers of LSPs, VPN instances (VRFs or VCs), and routes is important to determine when sizing the overall network.

- LSP setup rate: The rate at which LSPs can be set up is an important factor in overall network responsiveness.
- Signaling protocol scalability: The limits of an MPLS router running signaling protocols such as LDP or

RSVP-TE must be verified to determine the number of protocol sessions that can be sustained.

Together, these numbers will determine the quantity of routers that must be deployed for a given number of customers.

## Performance

One of the original proposed benefits of MPLS was the performance boost associated with switching on a label as opposed to routing on an IP address. While this is of less concern today, the forwarding performance of PE routers at the edge of the MPLS network still involves IP (or other) lookups and assignments. Vendors and service providers alike must test and characterize MPLS devices across multiple interface types (Ethernet, POS, ATM) for traditional data plane performance metrics:

- Data throughput
- Packet loss
- Latency
- Jitter

Given the advances in hardware-based routing in recent years, the expectations for device performance have grown so that line rate traffic support is typically a given. But the MPLS routers of today are being asked to perform many functions, with operational requirements at the data (traffic), control (routing), security, and management planes. With requirements for MPLS routers to run multiple protocols simultaneously, to interoperate among multiple technologies, and to apply QoS and other policies to traffic, the reality is that full performance is not a given.

Performance must be viewed in different usage scenarios, depending on how the network is designed and being operated.

Together, scalability and performance metrics can be competitive differentiators for equipment vendors. For service providers and network managers, they are a key selection criteria between vendors. Characterizing these elements is critical, since they directly impact the service quality that can be delivered to the end customer.

## Test Solution Requirements

MPLS test tools must be able to perform a wide variety of functions to test and validate MPLS devices and systems adequately. For conformance testing, the test solution must be able to fully exercise the control plane of the device or system under test. For performance and scalability testing, the test solution must be able to emulate MPLS routers at the control plane level and scale up for large capacity testing. And it must be able to drive traffic through the system at the data plane level to fully stress the device being tested.

**One of the original proposed benefits of MPLS was the performance boost associated with switching on a label as opposed to routing on an IP address.**

## Optimized hardware platform

While simple router emulations can be run on PCs or workstations, an optimized test system must be employed to provide complete testing capabilities and high levels of scalability. For example, to emulate a large network, a network interface on a test tool must support hundreds or even thousands of IP interfaces and MAC addresses—requirements that standard off-the-shelf hardware cannot support. Purpose-built test hardware is required to provide the flexibility and scalability needed to adequately test MPLS equipment.

## Routing protocol emulation

The test solution must be able to emulate the full range of routing protocols used in today's networks, including OSPF, IS-IS, RIP, and BGP. These routing protocols are used to advertise the underlying network topologies over which the MPLS network is established. In addition, traffic engineering extensions to these protocols, for example OSPF-TE and IS-IS-TE, must be supported to allow this aspect of MPLS to be tested.

## Signaling protocol emulation

MPLS signaling protocols must be supported to establish MPLS tunnels and signal L2 and L3 VPNs. Examples of these protocols include LDP, RSVP-TE, and MP-BGP. The test tool must be able to run these protocols simultaneously with the routing protocols on the same network interface.

## Traffic generation

Once the MPLS network has been established and all connections signaled, the test tool must be able to inject data traffic into the network topology, at speeds up to line rate, and it must be able to receive traffic as well. This means sending traffic over all of the LSPs configured on the test interfaces. On the receiving side, the test tool must be able to gather statistics and capture the traffic for analysis. An increasingly common requirement for test tools is to emulate real enterprise applications over the network. This allows for the characterization of the network in terms the end user really cares about, namely, how their applications will perform.

## Automation

Since MPLS testing involves complex setup and analysis requirements, tests must be repeatable, which makes automation very important. Scripting languages are normally used to provide automation in MPLS router testing. These tools enable quality assurance and manufacturing environments to perform repeatable regression tests necessary to ensure product functionality and quality.

# Ixia's Approach to MPLS Testing

## MPLS conformance testing

Ixia has addressed the challenges of protocol conformance testing by developing IxANVL (Ixia Automated Network Validation Library), the industry standard conformance test suite. While supporting over 30 protocols overall, IxANVL contains over 800 test cases to validate routers for MPLS label encapsulation, and LDP and RSVP-TE protocol conformance. IxANVL provides positive as well as negative test cases against the RFCs that specify these standards. Negative tests help validate device response to “killer packets.”

IxANVL performs its tests as a dialog: it sends packets to the router being tested, receives the packets sent in response, and then analyzes the response to determine the next action to take. This allows IxANVL to test complicated situations or reactions in a much more intelligent and flexible way than can be done by simple packet generation and capture devices.

IxANVL can run on standalone workstations or on Ixia test hardware. Its operation can be completely automated using a scripting interface. IxANVL source code is also available to users for customization, allowing a great degree of testing flexibility.

## MPLS scalability and performance testing

The general methodology employed by Ixia for testing the scalability and performance of MPLS routers involves first surrounding the device or system under test (DUT/SUT) with Ixia hardware test interfaces. The Ixia system then emulates everything else needed to test the device, including other MPLS routers, IP route injection, LSP signaling, and traffic transmission. In this way, large and complex topologies can be simulated to test the DUT/SUT in realistic system environments, with a minimum of hardware requirements. As an example, in Figure 6, four Ixia test interfaces are connected to the DUT with numerous routers being emulated per interface.

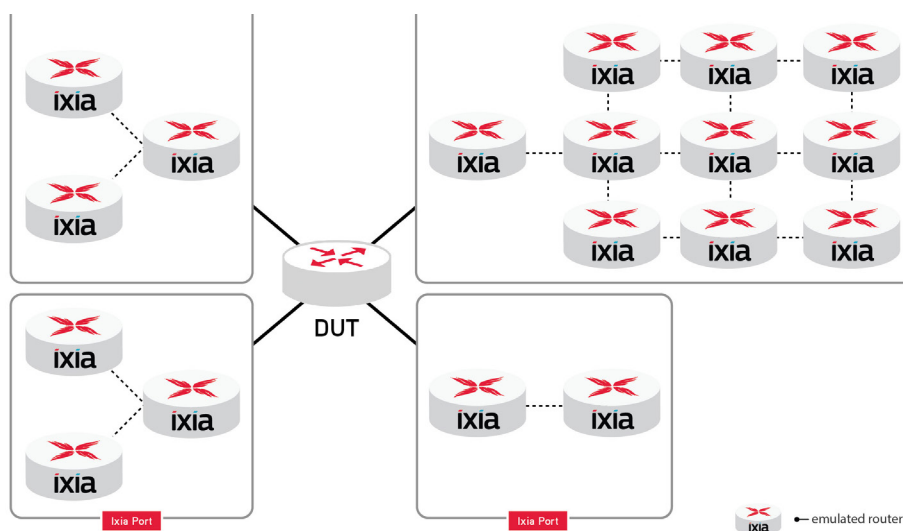


Figure 6. Ixia router simulation.

The general methodology employed by Ixia for testing the scalability and performance of MPLS routers involves first surrounding the device or system under test (DUT/SUT) with Ixia hardware test interfaces.

Ixia has developed two primary applications for MPLS performance testing, IxExplorer and IxScriptMate, each with a distinct testing focus.

**IxExplorer.** IxExplorer provides a high level of flexibility and functionality in protocol emulation, traffic generation, and analysis. IxExplorer is the primary controlling application for Ixia's purpose-built hardware test platform, allowing detailed configuration of protocols and analysis of test results.

Within IxExplorer, a comprehensive set of IP routing and MPLS signaling protocols is supported, including OSPF, IS-IS, RIP, BGP, LDP, and RSVP-TE, as well as multicast protocols. IxExplorer controls the protocol's operation on Ixia's test hardware architecture, which supports a CPU running Linux on each test port. This dedicated emulation environment allows hundreds of MPLS routers to be emulated on each network interface. Up to hundreds of thousands of LSPs can be signaled from each interface. Line rate traffic can be generated over the established connections. Alternatively, Ixia's IxChariot product can be used to transmit emulated enterprise application traffic over the MPLS device or network being tested to measure end-to-end application response times.

**IxScriptMate.** IxScriptMate provides a framework for running automated test scenarios. Numerous test suites have been developed within the IxScriptMate environment for testing the session and circuit scalability, traffic throughput performance, latency, and failover recovery capabilities of MPLS routers. IxScriptMate simplifies the configuration process by defining a configuration for the test and displaying the relevant parameters for user input. Tests then run automatically, and the results are presented to the user. This is especially useful for L2 and L3 VPNs, where the test configuration can involve multiple protocols and complex traffic generation requirements.

## Conclusion

In the post-bubble economy, the most important objectives for service providers and carriers are to:

- reduce operating costs
- preserve existing services
- introduce new services efficiently

MPLS technology has proven its value for delivering new services while at the same time allowing migration from old to new networks. By converging new and legacy network services over an MPLS network, providers and carriers can introduce efficiencies that promise great savings in operating costs. As a result, MPLS is well into mainstream deployment in networks around the world as a standard backbone technology for converged networks.

However, MPLS has proven to be an extremely complex technology, encompassing a wide range of functionality and applications. Vendors who develop MPLS technology, as well as organizations looking to deploy MPLS, must consider the complexity of the technology, its continually evolving state, and its impact on network performance and scalability.

To manage the complexity of MPLS, a wide range of protocols, services, applications, and hardware must be tested and validated. For network managers and vendors of MPLS-related products and services, a comprehensive and well designed conformance and performance testing solution is crucial to the success of MPLS technology.

Ixia provides that solution with

- IxANVL, the industry standard conformance test suite
- IxExplorer and IxChariot, providing flexibility and functionality in protocol emulation, traffic generation, and analysis
- IxScriptMate, providing the efficiency of automated testing

Together, these tools enable the providers of next-generation MPLS products and services to ensure the reliability, performance, scalability, and profitability of their offerings.

**MPLS technology has proven its value for delivering new services while at the same time allowing migration from old to new networks.**

# Appendix: MPLS Testing Examples

This appendix contains several examples of brief MPLS test plans, with specific examples showing how Ixia's solutions address the challenges of MPLS testing.

## IxANVL LDP Conformance Test

**Objective:** To characterize the MPLS router's compliance with LDP RFC standards.

**Test setup:** IxANVL Linux workstation connected directly, or via Ixia test hardware, to DUT with two network connections — one for request packets and one for response packets.

**Methodology:** IxANVL runs a number of test cases against the DUT based on direct interpretation of the LDP RFCs 3036 and 3215.

1. Configure each IxANVL network interface with the appropriate network parameters, including those of the DUT such as IP address, MAC address, gateway, etc.
2. Specify configuration of the DUT, typically via command scripts such as Expect scripts.
3. Select the set of IxANVL LDP test cases to run during the test session (see Figure 7).
4. Run IxANVL in batch mode with the command scripts, reconfiguring the DUT as required between test cases to match the IxANVL test setup.

**Results:** Number of tests passed/failed, including reasons for failed cases (see Figure 8).

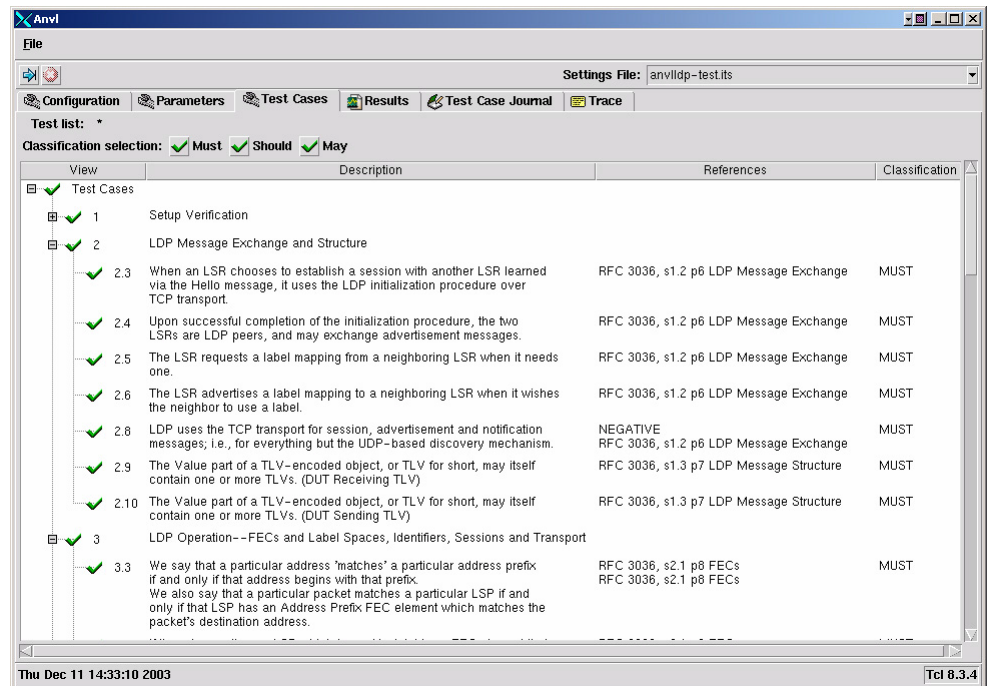


Figure 7. IxANVL LDP test cases

The screenshot shows the IxANVL test results window. The 'Results' tab is selected, displaying a table of test cases. The table has columns for Case name, Case status, Case start time, Elapsed time (ms), and Case comment. The test cases range from LDP-1.1 to LDP-1.25. Most cases are marked as 'PASS', but LDP-1.8 and LDP-1.25 are marked as 'FAIL' with specific error messages in the comments.

| Case name | Case status | Case start time     | Elapsed time (ms) | Case comment                                                      |
|-----------|-------------|---------------------|-------------------|-------------------------------------------------------------------|
| LDP-1.1   | PASS        | 2003-12-11 14:57:47 | 17887             |                                                                   |
| LDP-1.2   | PASS        | 2003-12-11 14:58:05 | 16995             |                                                                   |
| LDP-1.3   | PASS        | 2003-12-11 14:58:22 | 19322             |                                                                   |
| LDP-1.4   | PASS*       | 2003-12-11 14:58:41 | 24004             |                                                                   |
| LDP-1.6   | PASS        | 2003-12-11 14:59:05 | 31111             |                                                                   |
| LDP-1.7   | PASS        | 2003-12-11 14:59:36 | 23540             |                                                                   |
| LDP-1.8   | FAIL        | 2003-12-11 15:00:00 | 70395             | No Label Request message received from 10.1.3.11                  |
| LDP-1.9   | PASS        | 2003-12-11 15:01:10 | 23048             |                                                                   |
| LDP-1.12  | PASS        | 2003-12-11 15:01:34 | 42139             |                                                                   |
| LDP-1.13  | PASS        | 2003-12-11 15:02:16 | 45993             |                                                                   |
| LDP-1.14  | PASS        | 2003-12-11 15:03:02 | 28299             |                                                                   |
| LDP-1.18  | PASS        | 2003-12-11 15:03:30 | 20304             |                                                                   |
| LDP-1.19  | PASS        | 2003-12-11 15:03:50 | 31257             |                                                                   |
| LDP-1.24  | PASS        | 2003-12-11 15:04:22 | 40109             |                                                                   |
| LDP-1.25  | FAIL        | 2003-12-11 15:05:02 | 58541             | Did not receive Label Mapping Message from 10.1.3.11 for FEC 10.1 |

At the bottom of the window, it says 'MPLS Test Suites/LDP/ complete' and 'Tcl 8.3.4'.

Figure 8. IxANVL LDP test results.

## IxScriptMate L2 VPN Partial Mesh Performance Test

**Objective:** To determine the maximum rate an LSR configured as an L2 VPN PE router can “push” MPLS labels onto incoming Layer 2 packets and forward the resulting MPLS traffic, or “pop” labels from incoming MPLS packets and forward the resulting Layer 2 traffic with no loss.

**Test setup:** Minimum of two Ixia ports connected to the DUT — one to simulate a PE router and another to simulate a CE router. Additional ports can be configured to emulate multiple PEs/CEs (see Figure 9). The IxScriptMate application, running on a workstation, controls the test running on Ixia hardware.

**Parameters:** Number of PEs/CEs, number of VCs per PE, VC distribution style (consecutive or round robin), frame size distribution, traffic transmission rate.

### Methodology:

1. Each Ixia port simulating a PE router establishes an OSPF session, LDP session, and Extended LDP (Martini) session with the DUT.
2. If more than one Ixia port is being used to simulate PE routers, the VC IDs can be distributed among them in either round robin or consecutive fashion.
3. The CE and/or PE ports transmit traffic at the specified rate. If frame loss occurs, the transmission rate is alternately reduced/increased using a binary search algorithm to determine the maximum rate at which the DUT can forward traffic without loss.

**Results:** Frame loss, latency, data errors, sequence errors.

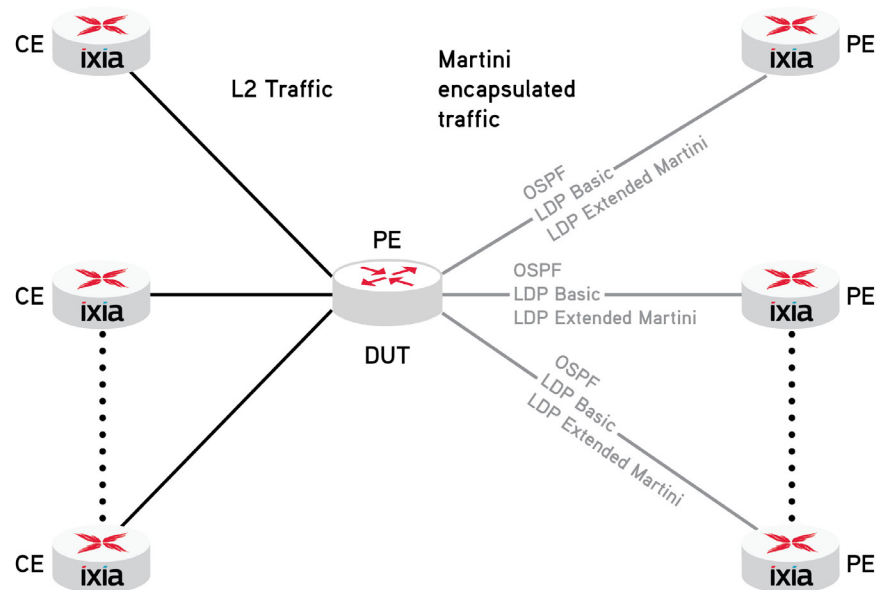


Figure 9. Test setup

## IxScriptMate L3 VPN RSVP-TE Egress Performance

**Objective:** To determine the maximum rate an LER configured as an L3 VPN PE router can “pop” MPLS labels from incoming packets and forward the resulting IP traffic with no loss.

**Test setup:** Two Ixia ports connected to the DUT — one to simulate a PE and P router and another to simulate a CE router (see Figure 10).

**Parameters:** OSPF parameters, BGP parameters, number of routes per CE, frame size distribution, traffic transmission rate.

### Methodology:

1. The port simulating the PE/P router establishes an OSPF session with the DUT and advertises the loopback address of the simulated PE router. Traffic engineering parameters are advertised using OSPF-TE.
2. Bidirectional LSPs are established using RSVP-TE.
3. A Multi-Protocol internal BGP (MP- iBGP) session is established with the DUT.
4. The port simulating the PE router transmits MPLS traffic at the specified rate. If frame loss occurs, the transmission rate is alternately reduced/increased using a binary search algorithm to determine the maximum rate at which the DUT can forward traffic without loss.

**Results:** Transmit rate, latency, data errors, sequence errors.

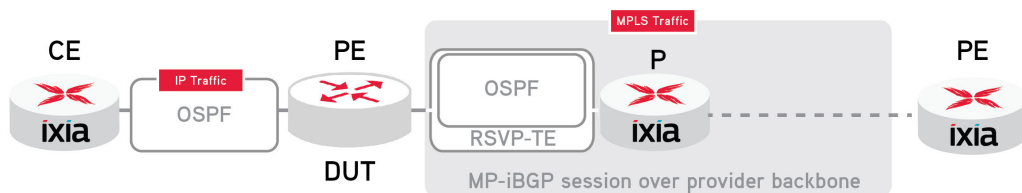


Figure 10. IxScriptMate L3 VPN RSVP-TE egress performance.

## IxExplorer LDP Extended Martini Session Scalability Test

**Objective:** To determine the maximum number of LDP Extended Martini sessions the DUT can sustain at one time.

**Test setup:** One Ixia port connected to the DUT (see Figure 11).

**Methodology:**

1. An OSPF session is established with the DUT.
2. An LDP basic session is established with the DUT, advertising the Ixia port loopback address as a FEC.
3. A number of LDP Extended Martini sessions (based on test expectations) are established with the DUT with one or more Layer 2 VC FECs advertised per session.
4. Status on the port is monitored to determine if all configured sessions are successfully established. Figure 14 shows the MPLS Martini labels learned by IxExplorer from the DUT — one for each session.
5. If all sessions are successfully established, the number of extended sessions configured is increased and the test rerun. If not all are established, the number of sessions is lowered and the test repeated.

**Results:** LDP Extended Martini session capacity.

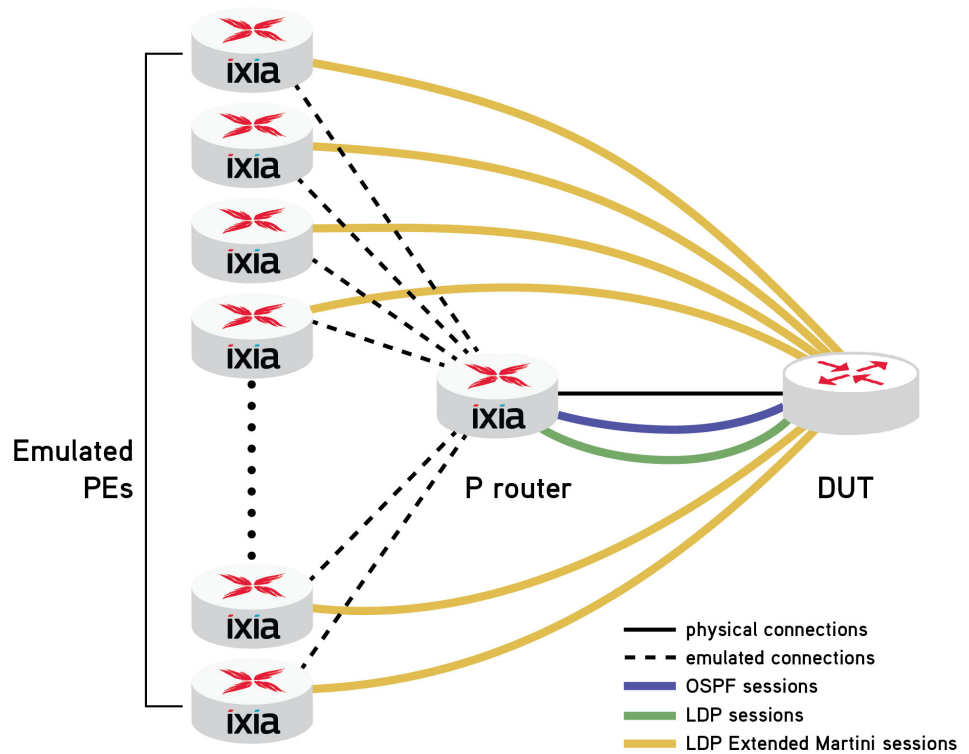


Figure 11. IxExplorer LDP Extended Martini session scalability test setup 4

ProtocolSelect

Protocol Interfaces

IP

ARP

BGP

OSPF

OSPFv3

ISIS

RSVP-TE

LDP

loopback:02:01

loopback:08:03 Running

loopback:08:04 Running

RID - 8.4.0.0

RID - 4.4.5.250

LDP Interfaces

4.4.5.250

Learned Labels

Advertising FEC Ranges

Explicit Include

L2 VC FECs

loopback:09:03

loopback:09:04

RIP

RIPng

IGMP

MLD

PIM-SM

Stream Generation Map

Number of Labels 400

Refresh

Filter

Learned Martini Labels

|    | Peer     | Label Space ID | VC Type | Group ID | VC ID | Label | PW State | C Bit | MTU   |
|----|----------|----------------|---------|----------|-------|-------|----------|-------|-------|
| 1  | 4.4.4.1  | 0              | VLAN    | 1        | 1     | 201   | Up       |       | 1,500 |
| 2  | 4.4.4.2  | 0              | VLAN    | 1        | 2     | 202   | Up       |       | 1,500 |
| 3  | 4.4.4.3  | 0              | VLAN    | 1        | 3     | 203   | Up       |       | 1,500 |
| 4  | 4.4.4.4  | 0              | VLAN    | 1        | 4     | 204   | Up       |       | 1,500 |
| 5  | 4.4.4.5  | 0              | VLAN    | 1        | 5     | 205   | Up       |       | 1,500 |
| 6  | 4.4.4.6  | 0              | VLAN    | 1        | 6     | 206   | Up       |       | 1,500 |
| 7  | 4.4.4.7  | 0              | VLAN    | 1        | 7     | 207   | Up       |       | 1,500 |
| 8  | 4.4.4.8  | 0              | VLAN    | 1        | 8     | 208   | Up       |       | 1,500 |
| 9  | 4.4.4.9  | 0              | VLAN    | 1        | 9     | 209   | Up       |       | 1,500 |
| 10 | 4.4.4.10 | 0              | VLAN    | 1        | 10    | 210   | Up       |       | 1,500 |
| 11 | 4.4.4.11 | 0              | VLAN    | 1        | 11    | 211   | Up       |       | 1,500 |
| 12 | 4.4.4.12 | 0              | VLAN    | 1        | 12    | 212   | Up       |       | 1,500 |
| 13 | 4.4.4.13 | 0              | VLAN    | 1        | 13    | 213   | Up       |       | 1,500 |
| 14 | 4.4.4.14 | 0              | VLAN    | 1        | 14    | 214   | Up       |       | 1,500 |
| 15 | 4.4.4.15 | 0              | VLAN    | 1        | 15    | 215   | Up       |       | 1,500 |
| 16 | 4.4.4.16 | 0              | VLAN    | 1        | 16    | 216   | Up       |       | 1,500 |
| 17 | 4.4.4.17 | 0              | VLAN    | 1        | 17    | 217   | Up       |       | 1,500 |
| 18 | 4.4.4.18 | 0              | VLAN    | 1        | 18    | 218   | Up       |       | 1,500 |
| 19 | 4.4.4.19 | 0              | VLAN    | 1        | 19    | 219   | Up       |       | 1,500 |
| 20 | 4.4.4.20 | 0              | VLAN    | 1        | 20    | 220   | Up       |       | 1,500 |
| 21 | 4.4.4.21 | 0              | VLAN    | 1        | 21    | 221   | Up       |       | 1,500 |
| 22 | 4.4.4.22 | 0              | VLAN    | 1        | 22    | 222   | Up       |       | 1,500 |

Figure 12. Test results (learned labels)

# IxScriptMate VPLS MAC Address Cache Capacity Test

**Objective:** To determine the maximum capacity of a router's Layer 2 MAC address cache.

**Test setup:** A minimum of three Ixia test ports connected to the DUT — a Test port, a Monitoring port, and a Learning port.

**Parameters:** Number of PEs per port, number of VPLS instances per CE, number of hosts per VLAN, DUT MAC address table size, DUT MAC address aging time. (See Figure 13.)

## Methodology:

1. OSPF and LDP are run based on user-configured parameters to set up the network topology and signal the VPLS instances.
2. Learning frames, equal in number to the specified DUT MAC address table size, are sent to the Learning port. These frames contain varying source MAC addresses and a fixed destination MAC address corresponding to the address connected to the Test port.
3. Validation frames are sent to the Test port back to the addresses learned on the Learning port.
4. The Monitoring port listens for flooded or mis-forwarded frames from the DUT.
5. A binary search algorithm is used to determine the maximum number of addresses that can be learned without flooding or dropping frames.

**Results:** Maximum MAC address capacity total and per VPLS instance. (See Figure 14.)

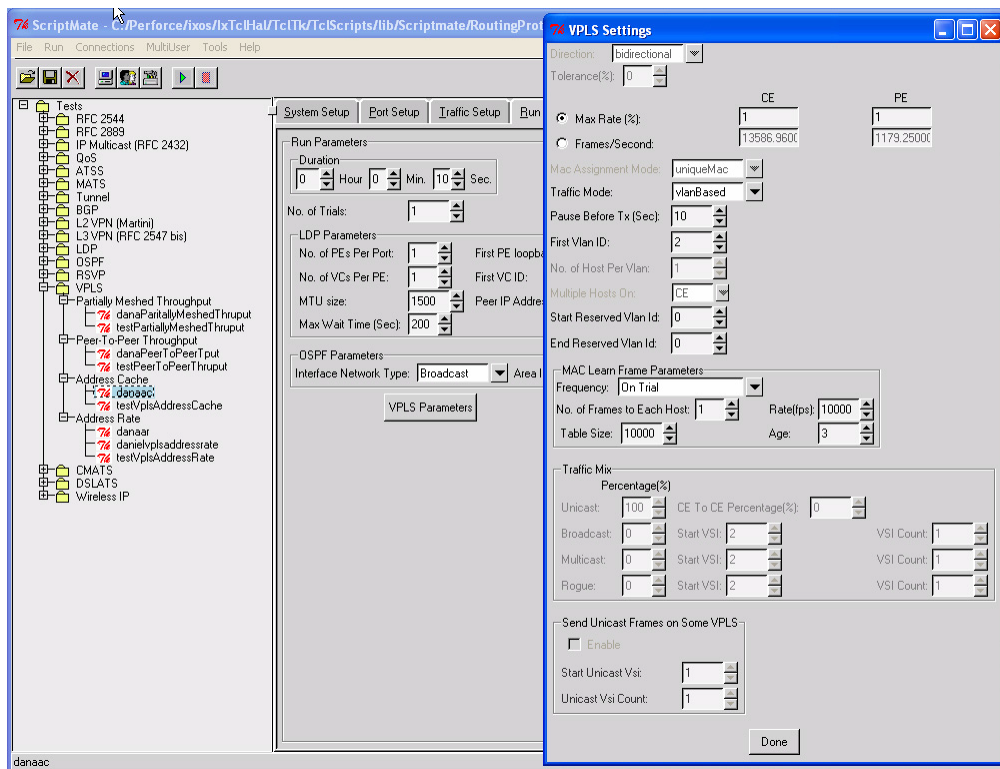


Figure 13. IxScriptMate run setup

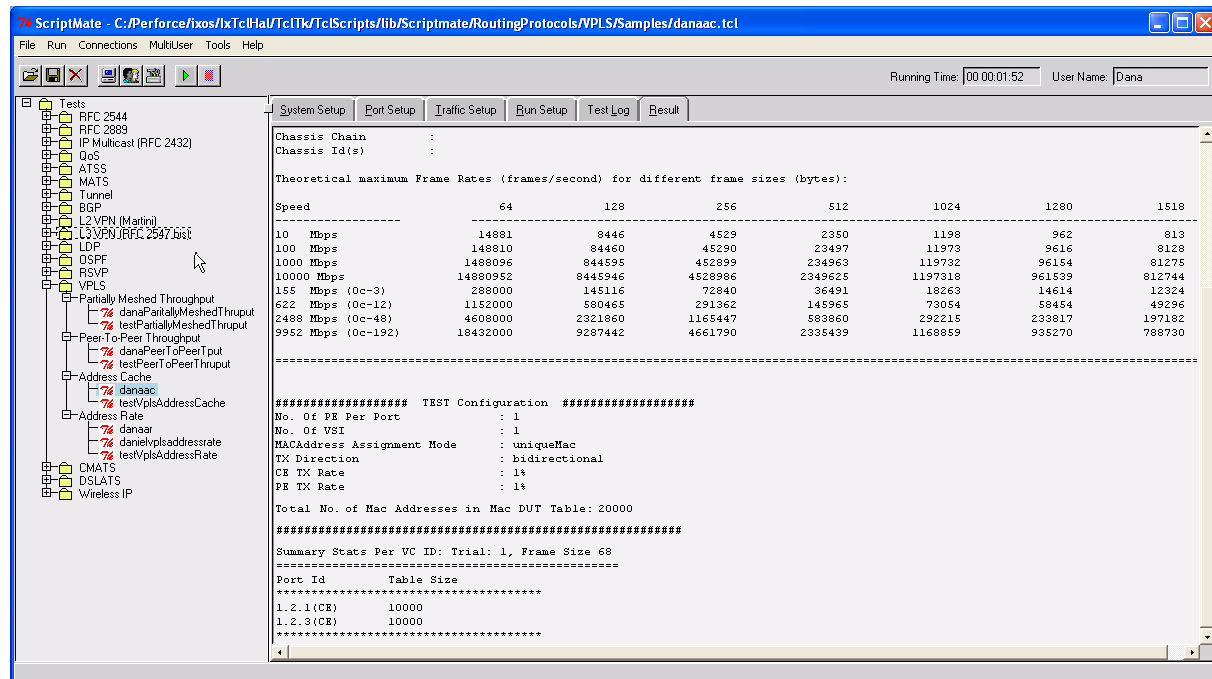


Figure 14. IxScriptMate test results

## IxExplorer RSVP-TE Fast Reroute Test

**Objective:** To measure the LSP switchover time of a router running RSVP-TE Fast Reroute between a primary LSP and a detour LSP upon link failure.

**Test setup:** Three Ixia test ports connected to the DUT — one acting as the ingress and two as egress (primary and detour). See Figure 15.

### Methodology:

1. Two bidirectional LSPs are signaled using RSVP-TE through the DUT from the Ixia ingress and egress ports.
2. RSVP-TE Fast Reroute objects are signaled to establish one LSP as a primary and the second LSP as a detour.
3. Unicast traffic is sent from the ingress port over the primary LSP.
4. A switchover to the detour LSP is initiated by bringing down the link to the DUT on the primary LSP.
5. Traffic is captured on both the egress ports. The switchover time is calculated by comparing the timestamp of the last packet received on the primary port with the timestamp of the first packet received on the detour port.

**Results:** Fast Reroute switchover time of the DUT.

Figure 15. IxScriptMate run setup

# Glossary

## Border Gateway Protocol (BGP)

An exterior gateway protocol defined in RFC 1267 and RFC 1268. BGP is the principal protocol used along the Internet backbone and within larger organizations.

## Constraint-Based Routing

Routing that uses intelligent path computation and explicit route specification to determine routes. This differs from typical non-Constraint-Based Routing, in which routes are calculated based only on shortest path. Constraint-Based Routing enables traffic engineering in MPLS networks.

## Class of Service (CoS)

Class of Service (CoS) is a method for managing network traffic by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.

## Customer Edge Router (CE)

A router at the edge of a customer network, the CE interfaces to a corresponding Provider Edge (PE) router at the edge of the service provider's network.

## Diffserv (Differentiated Services)

An architecture for providing different types or levels of service for network traffic.

## Exterior Gateway Protocol (EGP)

A protocol that distributes routing information to the routers that connect networks.

## Fast Reroute

A mechanism used in MPLS networks to provide redundant data paths for recovery from node or link failures. The RSVP-TE protocol is used to signal Fast Reroute configuration.

## Forward Equivalency Class (FEC)

A classification of a group of packets — all packets assigned to a FEC receive the same routing treatment. FECs can be based on IP address prefixes or service requirements for a type of packet (QoS, VPN, Traffic Engineering, etc.).

## Forwarding Information Base (FIB)

A table containing the information necessary to forward IP data in a router. At a minimum, the FIB contains the outbound interface identifier and next hop information for each reachable IP destination network.

## Internet Gateway Protocol (IGP)

Protocol that distributes routing information to the routers within a network. The term "gateway" is historical; "router" is currently the preferred term. Example IGPs are OSPF, IS-IS and RIP.

## IS-IS

An OSI/IP routing protocol, IS-IS stands for Intermediate System to Intermediate System (i.e., router to router). MPLS traffic engineering parameters can be distributed with IS-IS using extensions to the protocol (IS-IS-TE).

## L2 VPN

An emulation of a Layer 2 switching environment, supplied by a service provider for its customers, via a core network. In MPLS networks, L2 VPNs use LDP to signal connections for transporting Layer 2 frames over MPLS.

## L3 VPN

An emulation of Layer 3 services/distribution of routes, supplied by a service provider for its customers, via a core network. L3 VPNs use BGP extensions to signal provider-provisioned VPNs per IETF Draft RFC 2547bis.

## Label Distribution Protocol (LDP)

A protocol, defined in RFC 3036, used to distribute MPLS label and stream mapping information.

## Label Edge Router (LER)

A router at the edge of an MPLS network. At the ingress side, an LER maps IP packets to LSPs, adds the appropriate MPLS header, and forwards the packet to the next hop. At the egress side, an LER strips the MPLS label(s) and forwards the packet using traditional routing mechanisms.

## Label Information Base (LIB)

A table that specifies how to forward a packet in an MPLS router. This table associates each label with its corresponding FEC.

## Label Switched Path (LSP)

In MPLS, a path through a network from an ingress to an egress router that has been established through the distribution of labels that define hop-by-hop forwarding treatment.

## Label Switching Router (LSR)

A router, operating in the core of an MPLS network, that switches traffic based on labels.

## Martini Drafts

A set of IETF draft specifications (named for primary author Luca Martini) that define the mechanisms for creating Layer 2 MPLS VPNs. Such VPNs support Layer 2 traffic such as Frame Relay, ATM, and Ethernet tunnels over an MPLS network.

## Open Shortest Path First (OSPF)

A link-state routing protocol used by IP routers located within a single Autonomous System (AS) to determine routing paths. MPLS traffic engineering parameters can be distributed with OSPF using extensions to the protocol (OSPF-TE).

## **P Router (Provider Router)**

A router that operates in the core of an service provider network.

## **Provider Edge Router (PE)**

A router that operates at the edge of a service provider's network, interfacing with the corresponding Customer Edge (CE) router(s) at the edge of one or more customer networks.

## **Quality of Service (QoS)**

A measure of performance for a transmission system that reflects its transmission quality and service availability. QoS mechanisms provide the ability to manage network traffic's bandwidth, delay, and congestion.

## **Resource Reservation Protocol — Tunneling Extensions (RSVP-TE)**

Extensions to the RSVP protocol related to traffic engineering. RSVP-TE implements an assignment of labels from ingress to egress routers, with consideration for bandwidth and other QoS requirements.

## **Routing Information Protocol (RIP)**

An Internet routing protocol that uses hop count as a routing metric. RIP is the most common IGP used in the Internet.

## **Traffic Engineering**

Techniques and processes that optimize the routing of network traffic. Traffic engineering mechanisms enable network administrators to manage network traffic's bandwidth, delay, and congestion.

## **Virtual Circuit (VC)**

A circuit or path between points in a network that appears to be a discrete, physical path but is actually part of a managed pool of resources from which specific circuits are allocated as needed to meet traffic requirements.

## **Virtual Private LAN Service (VPLS)**

A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. The goal of VPLS is to provide a protocol-transparent, any- to-any, full-mesh service across a WAN.

## **Virtual Routing and Forwarding (VRF) Table**

A VPN routing/forwarding instance. A VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

